- **Expediente Nº: E/01284/2021**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: La reclamación interpuesta por ***A.A.A.*** (en lo sucesivo, parte reclamante) tiene entrada con fecha 15 de octubre de 2020 en la Agencia Española de Protección de Datos. La reclamación se dirige contra CONSEJERIA DE SANIDAD DE LA COMUNIDAD DE MADRID con NIF S7800001E (en adelante, parte reclamada).

Los motivos en los que basa su reclamación son: que solicitó acceso a su documentación clínica y le han sido entregados dos informes médicos de terceras personas y un CD del que desconoce si los datos que contiene son suyos, por lo que ha presentado reclamación en el hospital.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), con número de referencia E/09096/2020, se dio traslado de dicha reclamación a la parte reclamada el 10 de noviembre de 2020, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

No consta en esta Agencia contestación al traslado de la reclamación.

TERCERO: Con fecha 15 de enero de 2021 se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

Hechos según manifestaciones de la parte reclamante:

La parte reclamante manifiesta que tras solicitar al Centro de Salud Vicente Soldevilla el resultado de dos resonancias magnéticas a las que se había sometido con anterioridad le entregaron los informes de dos personas (terceros) ajenos a él con los siguientes datos personales de éstos: *"nombre, apellidos, fecha de nacimiento y resultado de unas resonancias magnéticas, entre otros datos".*

Fecha en la que tuvieron lugar los hechos reclamados:

Según la documentación provista por la parte reclamante, la entrega de la información de terceros se le habría efectuado con fecha de 18 de octubre de 2019.

Documentación relevante aportada por la parte reclamante:

- Informe de la Unidad Central de Radiodiagnóstico del Hospital de Tajo (Aranjuez) de fecha 12 de noviembre de 2016 que refiere los resultados de una prueba médica realizada a una tercera persona distinta de la parte reclamante.

- Informe de la Unidad Central de Radiodiagnóstico del Hospital de Tajo (Aranjuez) de fecha 19 de noviembre de 2016 que refiere los resultados de una prueba médica realizada a una tercera persona distinta de la parte reclamante.

- Solicitud de acceso a información clínica realizada el 7 de agosto de 2019 por la parte reclamante mediante el modelo de formulario a estos efectos del Hospital Universitario Infanta Leonor en el que solicita el resultado de las resonancias magnéticas efectuadas el 29 de junio de 2019 en el *"H. del Henares".* El impreso incluye la anotación manuscrita *"Recogida 18/10/2019".*

- Reclamación presentada por la parte reclamante con fecha 13 de octubre de 2020 mediante el modelo de formulario a estos efectos del Hospital Universitario Infanta Leonor en la que manifiesta que tras realizarse el día 29 de junio de 2019 dos resonancias magnéticas en *"H. Henares"*, el día 7 de agosto de 2019 solicitó el resultado de las mismas. Añade que *"el otro día me di cuenta"* de que los resultados que le habían facilitado correspondían a dos terceros. La reclamación incluye sello de fecha 13 de octubre de 2020 del *"Hospital Virgen de la Torre. S.A.P-C.E.P VICENTE SOLDEVILLA"* con reseña del número de expediente *"VS 163/10-20".*

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Además de la documentación aludida en el apartado de antecedentes, se recoge información de las siguientes fuentes:

- Escrito procedente del Comité Delegado de Protección de Datos (en adelante, CDPD) de la parte reclamada *"en su calidad de interlocutor de la Consejería de Sanidad de la Comunidad de Madrid con esta Agencia, acorde a lo establecido en el artículo 37.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)"* y registrado de entrada en la AEPD con fecha de 29 de julio de 2021 y número O00007128e2100033077 (Escrito1).

La parte reclamada adjunta al Escrito1 el *"INFORME A LA RECLAMACIÓN VS163/10-20 DE D.* ***A.A.A.*** *EN RELACIÓN A LA ENTREGA DE DOCUMENTACION CLINICA (CD DE RMN DE CEREBRO Y COLUMNA CERVICAL ASI COMO SUS*

CORRESPONDIENTES [SIC] INFORMES)" emitido por la Directora Gerente del Hospital Universitario Infanta Leonor a petición del CDPD. En este informe se consigna la siguiente información de relevancia a los efectos de la presente investigación:

"1.- Descripción de los hechos ocurridos y de las acciones tomadas con objeto de minimizar los efectos adversos generados por la brecha de seguridad.

- *Que con fecha 7 de agosto de 2019 D.* ***A.A.A.*** *realizo [sic] una Solicitud de Acceso a Documentación Clínica en el Servicio de Atención al Paciente.*

- *Desde el Servicio de Atención al Paciente se contacta con el Servicio de Diagnóstico por Imagen que recibe copia de la solicitud de documentación clínica y copia de la nota de cita de la prueba con indicación del tipo de prueba, lugar de realización, día y hora de la misma y nombre del paciente y apellidos del paciente. El acceso a las imágenes y copias de la misma es personalizado.*

- *El Servicio de Diagnóstico por Imagen, realiza la copia de las imágenes (C.D.) de la prueba entregando dicho C.D. al Servicio de Atención al Paciente.*

- *Una vez recabada toda la información (C.D. e informe de la prueba) por el Servicio de Atención al Paciente se pone dentro de un sobre a nombre del paciente y número de expediente y es lacrado.*

- *El paciente fue avisado de que podía pasar a recoger la documentación solicitada.*

- *Con fecha 18 de octubre de 2019, tras dos meses, fue recogida dicha documentación por el paciente.*

- *Con fecha 13 de octubre de 2020 interpuso una reclamación con número de evento 58581/20 y número de registro VS163/10/20 y registro de salida de la contestación el 19 de octubre de 2020.*

- *El día que el paciente puso la reclamación, 13 de octubre de 2020, vino por ventanilla de Admisión diciendo que había recibido dos informes de resonancias de otras pacientes, la compañera que le atendió le informó que esos informes no se le habían dado allí pues no coincidían con el modelo que habitualmente se emite; y se quedó con los informes al ser el Centro de especialidades el custodio de la documentación clínica y no pertenecer al reclamante.*

- *No estando de acuerdo el paciente, la compañera de Admisión llamó a la compañera de Atención al Paciente quien corroboro [sic] la actuación de la primera. Ante la duda que tenía el paciente de que las imágenes e informe de CD fueran las suyas, se le propuso que lo trajera para despejar sus dudas, hecho que a fecha de hoy no ha sucedido.*

- *El Servicio de Atención al Paciente del Centro de Especialidades de Vicente Soldevilla informa que desconoce el origen de los informes de Resonancias Magnéticas de las pacientes que indica en el escrito de reclamación. Ya que como hemos podido comprobar no aparece identificado la persona que accedió a dichos informes y en nuestro centro el sistema siempre identifica al solicitante.*

- *El acceso a los informes de resonancias se realiza a través de la aplicación HORUS. Teniendo, el profesional, que identificarse con su clave de usuario y contraseña y una vez dentro de la aplicación hay que identificar al paciente para recabar la información solicitada.*

- *Los informes que se sacan de la aplicación HORUS en su encabezamiento llevan el nombre del profesional que ha accedido a dicha aplicación.*

- *Los informes que aporta el reclamante carecen de dicha identificación, los informes nunca se grapan ni se rotulan. Situación que se da en los entregados por el reclamante.*

- *Los informes que aporta el reclamante NO han salido del centro de Especialidades Vicente Soldevilla al no tener el formato habitual establecido para este centro.*

2.- Especificación de las causas que han originado la brecha de seguridad, incluyendo la información sobre las condiciones existentes que posibilitaron la misma. Incluir la descripción de las medidas de seguridad implantadas con anterioridad para dichos tratamientos y motivo por el cual no impidieron la brecha de seguridad.

A la vista de los descrito en el primer punto, se desestima la posibilidad de que haya existido una brecha de seguridad. Las medidas de seguridad no se han modificado y las medidas del tratamiento de la información sigue siendo la misma, al no haberse generado brecha.

3.- Determinación del número de afectados (con indicación de si es real o estimado) por el problema origen que causa la brecha de seguridad y de las categorías de datos personales afectadas.

No se considera que haya ningún afectado por no producirse brecha de seguridad según los hechos comentados.

4.- Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo de los que tenga constancia. Evaluación de las posibles consecuencias para los afectados.

Los hechos no son recurrentes pues se extrema el tratamiento de la documentación y datos clínicos de los pacientes con la mayor eficiencia.

5.- Descripción de las medidas tomadas para corregir la brecha de seguridad y de las adoptadas para evitar que ocurra nuevamente.

No se han tomado medidas según lo referido en los puntos anteriores.

6.- Indicación, en su caso, de si tiene constancia de la utilización por terceros de los datos personales obtenidos a través de la brecha de seguridad o de su publicación en internet. En tal caso se solicita la aportación de las evidencias de que disponga al respecto.

Desconocemos si el reclamante ha utilizado los datos que indica le fueron entregados y retirados inmediatamente por el personal que trata la documentación.

7.- Información, en su caso, respecto a la notificación realizada a los afectados por la brecha de seguridad. Facilitar, en tal caso, copia de la notificación remitida y del procedimiento de remisión.

No hay afectados, salvo incidencias no conocidas referidas en el punto 6.

8.- En caso de que el mantenimiento de los Sistemas de Información afectados por la brecha sea realizado por terceras compañías incluir copia del contrato suscrito al efecto (encargado y subencargado del tratamiento). Incluir comunicaciones mantenida [sic] con dichas compañías para la resolución de la brecha.

No hay terceras compañías afectadas.

9.- Motivo por el cual no se ha notificado a la AEPD la brecha de seguridad.

No se notificó porque no se entendió la presunta entrega de la documentación como un problema de seguridad. Al no haberse entregado en nuestro centro según la información objetiva que disponemos.

Llama la atención el tiempo de decalaje desde la recepción de la información a la interposición de la reclamación."

La parte reclamada añade, en el Escrito1, que ha solicitado *"en razón a las competencias que ostenta, información a la Gerencia Asistencial de Atención Primaria (GAAS)"*. Así, manifiesta al respecto que ésta habría analizado la información del reclamante y de los otros dos pacientes afectados llegando a la siguiente conclusión: *"no encontramos anotaciones, imágenes ni informes de ninguno de los pacientes referidos en las historias clínicas de los otros, no habiéndose insertado ni facilitado datos no correspondientes a nivel de Atención Primaria".*

Además, la parte reclamante expresa en el Escrito1 que *"se ha requerido, en razón a las competencias que ostenta, a la Dirección General de Sistemas de Información y Equipamientos Sanitarios (DGSIES) que compruebe la información que se visualiza en el perfil de HORUS del reclamante"*. Así, añade que *"la DGSIES ha confirmado que en perfil de HORUS de D.* ***A.A.A.*** *no se visualiza ningún informe que no corresponda al paciente."*

Por último, la parte reclamada señala en el Escrito1 lo siguiente: *"No obstante lo anterior, se ha decidido seguir realizando investigaciones internas, en cumplimiento*

del principio de responsabilidad proactiva, con la finalidad de detectar posibles riesgos de seguridad y aplicar medidas técnicas y organizativas apropiadas. En caso de que se aparezcan evidencias de la existencia de una brecha de seguridad, se notificaría la misma en tiempo y forma a la Agencia Española de Protección de Datos, cuando sea probable que la brecha constituya un riesgo para los derechos y libertades de las personas. Asimismo, se notificaría a los interesados si se considera que puede suponer un alto riesgo para los derechos y libertades de las personas físicas".

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante quiebra de seguridad) como "todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos." En el presente caso, consta que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, al haberse producido un acceso no autorizado a historias clínicas.

III

El artículo 5.1.f) del RGPD, que recoge los "Principios relativos al tratamiento", dispone: "1. Los datos personales serán: f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (integridad y confidencialidad").

IV

La seguridad del tratamiento viene regulada en el artículo 32 del RGPD, que establece:

"Seguridad del tratamiento

Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales.

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

V

La CONSEJERIA DE SANIDAD DE LA COMUNIDAD DE MADRID ha informado sobre las medidas de seguridad existentes para el acceso de sus trabajadores a los informes de resonancias que se realiza a través de la aplicación HORUS. Teniendo el profesional que identificarse con su clave y numero de usuario y contraseña y una vez dentro hay que identificar al paciente para recabar la información solicitada. También recalca que estos informes que sacan de la aplicación HORUS en su encabezamiento llevan el nombre del profesional que ha accedido a dicha aplicación. Los informes que aporta la parte reclamante carecen de dicha identificación.

La CONSEJERIA DE SANIDAD ha decidido seguir realizando investigaciones internas, en cumplimiento del principio de responsabilidad proactiva, con la finalidad de detectar posibles riesgos de seguridad y aplicar medidas técnicas y organizativas apropiadas. En caso de que aparezcan evidencias de la existencia de una brecha de

seguridad, se notificaría la misma en tiempo y forma a la Agencia Española de Protección de Datos, cuando sea probable que la brecha constituya un riesgo para los derechos y libertades de las personas. Asimismo, se notificaría a los interesados si se considera que puede suponer un alto riesgo para los derechos y libertades de las personas físicas.

A la vista de la información remitida por la parte reclamante, consta que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, pero no se ha podido probar que el origen de los documentos que aporta el reclamante haya sido entregado por la CONSEJERIA DE SANIDAD, puesto que según alegan tienen medidas para controlar las impresiones. El contenido del CD al que hace referencia la parte reclamante se desconoce al no haber aportado información sobre su contenido.

En definitiva, según el artículo 53.2.b) de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, que reconoce al interesado el derecho “A la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario”, impide imputar una infracción administrativa cuando no se hayan obtenido evidencias o indicios de los que se deriven la existencia de infracción.

En el presente caso, no ha sido posible determinar al responsable del acceso indebido a los informes médicos de terceras personas, a pesar de los intentos realizados por la Inspección de Datos, cuyo detalle consta reseñado en los Antecedentes de esta Resolución.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a ***A.A.A.*** y a la CONSEJERIA DE SANIDAD DE LA COMUNIDAD DE MADRID.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción

Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

940-010921

Mar España Martí
Directora de la Agencia Española de Protección de Datos